REMARKS

Applicant has amended the specification to reference designations and replace them with "(not shown)" since the attacking computer and the ISP are not shown nor are they needed to be shown in FIG. 1.

The examiner objected to claims 2-3, 5, and 7-8, because of the use of 'hardened" being inconsistent with claim 1. Applicant has corrected claims 2 and 3.

The examiner rejected claims 1-36 under 35 U.S.C. 103(a), as being unpatentable over Fletcher et al., U.S. Pat. No. 6,108,782, (Fletcher), in view of Cox U.S. Pat. No. 6,738,814, (Cox).

The examiner stated:

> **As per claims 1, 12, 15 and 28, '782 teaches the invention of a method and system for remote monitoring in a distributed environment comprising: a data center, any element that may come under attack, coupled to a network (Lans, Wans etc.), monitoring traffic1 plurality of monitors (Rmon/probes/monitors/dRmons), disposed at a plurality of points (network devices, Is, hubs, switches, bridges, may also be any network device), communicating data from the monitors to a redundant network, and a central controller/dRmon collector (RMON-independent probe/monitor), collecting statistical data, performing analysis, and filtering (col. 4, lines 5-55, col. 6, lines 25-65 et seq., col. 7, lines 35 et seq., figs. 1 and 8), DRMON manager, (fig. 1, col. 4, lines 5 – 54 et seq., col.5, lines 1-10 et seq., and 50 -64 et seq., col. 6, lines 10 et seq., col. 7, lines 47 et seq., col. 8, lines 20-29 et seq., lines 45-55 et seq.), plural monitors and plural points/groups or domains (fig. 8, col. 6, lines 47 et seq., col. 7, lines 34-41 et seq., and col. 18, lines 51 et seq.) and collection across different networks (cols. 7, lines 35 et seq., and col. 8, lines 20-55 et seq., col. 9, lines 33 et seq., col. 13, lines 34 et seq., col. 20, lines 16 et seq.). Not explicitly taught is the rule set for the filtering and/or collection mechanisms being that to detect a denial of service attack.**
>
> **Cox teaches a method for blocking denial of service attack, comprising: a private (12) and public network (14), having a victim data center/point or object of attack (col. 1, lines 23 et seq.), and monitoring means to intelligently analyze the incoming packets (col. 1, lines 60-65 and col. 3, lines 25 et seq.). It would have been obvious to one of ordinary skill in the art at the time of the invention, to augment the invention of '782 with the programming means of '814 as a filtering or probe monitoring program. One of ordinary skill in the art would have been able to perform this modification by having a program, subroutine, or firmware installed in the dRmon's software of hardware monitoring/collecting modules. A person of ordinary skill in the art would have been motivated to perform such a modification because, '814 recites that there is an increasing pattern of denial attacks being performed at network routing devices (col. 1, lines 24-37). '782 teaches that it is desirable to have Rrnons implemented as independent distributed network probes, because of the advantages it offers in performance monitoring and enhanced remote monitoring (col. 4, lines 5-55 et seq., col. 20, lines 43 et seq.). A person of ordinary**

> **skill would have readily envisaged that the use of distributed Rmons, via programming of their filtering routines, could readily be programmed to detect potentially harmful packed, such as a denial of service attack. So that, by having distributed Rmons within a network systems that the potential for detecting malicious attacks would be greatly increase, and security of the system enhanced.**

Claims 1-36, as amended are allowable over Fletcher in view of Cox. Claim 1, for example, calls for a method of thwarting denial of service attacks on a victim data center coupled to a network. Claim 1 recites monitoring network traffic through monitors disposed at a plurality of points in the network and communicating data from the monitors to a central controller, with data sent from the monitors to the central controller over a redundant network that is a different network from the network being monitored. Neither Fletcher nor Cox disclose or suggest the combination of these features.

The examiner contends that Fletcher '782 discloses "... a data center, any element that may come under attack, coupled to a network (Lans, Wans etc.), monitoring traffic a plurality of monitors (Rmon/probes/monitors/dRmons), communicating data from the monitors to a redundant network, and a central controller/dRmon collector .... (See complete rejection above). Applicant contends that Fletcher '782 does not disclose "communicating data from the monitors to a central controller over a redundant network," as claimed.

Nowhere in Fletcher does one of ordinary skill in the art find any teaching that remotely suggests communicating data from the monitors to a central controller, over a redundant network that is a different network from the network being monitored. Fletcher does not describe nor suggest a central controller, nor does Fletcher describe or suggest communicating data from the monitors over a redundant network that is a different network from the network being monitored. In FIG. 1, Fletcher discloses that the collectors communicate data to other collectors over the network monitored by the collectors. For instance, Fletcher discloses:

> **In a LAN such as 40, data is generally transmitted between ESs as independent packets, with each packet containing a header having at least a destination address specifying an ultimate destination and generally also having a source address and other transmission information such as transmission priority. Packets are generally formatted according to a particular protocol and contain a protocol identifier of that protocol. Packets may be encased in other packets. FIG. 2 illustrates a packet.**

Fletcher does not describe nor suggest any other mechanism for communicating data from the collectors.

The examiner admits that Fletcher does not disclose or explicitly teach "the rule set for the filtering and/or collection mechanisms being that to detect a denial of service attack." The examiner relies on Cox for such teaching.

Cox fails to cure the above noted deficiencies in Fletcher. Cox discloses denial of service attacks and a technique to block attacks on a private network by a routing device interconnecting the private network (12) to a public network (14), and analyzing an incoming data packet from the public network (14) to match against known patterns where the known patterns are associated with known forms of attack on the private network (12). However, Cox's disclosure of a routing device interconnecting the private network to the public network, does not suggest any distributed arrangement. That is Cox fails to suggest "monitoring network traffic through monitors disposed at a plurality of points in the network" and "communicating data from the monitors to a central controller ***."

Moreover, as amended, claim 1 further distinguishes since Cox fails to suggest analyzing data including network traffic statistics to identify network traffic that is part of a denial of service attack; and filtering the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as part of the denial of service attack.

Cox also does not suggest nor would Cox have any use for an arrangement where data is sent from the monitors to the central controller over a redundant network that is a different network from the network being monitored, since Cox does not describe any distributed arrangement. In Cox, the network that is monitored, i.e., "the public network," carries data (i.e., packets). However, Cox does not disclose that the data comes from monitors, as in claim 1. Nonetheless, in Cox data (packets) and the traffic (same packets) travel over the same network (public network).

Cox likewise neither describes nor suggests analyzing network traffic statistics to identify network traffic that is part of a denial of service attack, since Cox seeks to match attack patterns

against know patterns of attack. Thus, one of the advantages of the distributed arrangement of claim 1 (as disclosed on page 4, line 11, of applicant's specification) is that:

> **The arrangement uses a distributed analysis emphasizing the underlying characteristics of a DoS attack i.e., congestion and slow server response to produce a robust and comprehensive DoS solution. Thus, this architecture 10 can stop new attacks rather than some solutions that can only stop previously seen attacks. Furthermore, the distributed architecture 10 will frequently stop an attack near its source, before it uses bandwidth on the wider Internet 14 or congests access links to the targeted victim 12.**

In contrast to Cox, which can only detect attacks that match some pattern, claim 1 provides a distributed arrangement that can detect new attacks because:

> **All deployed devices e.g., gateways 26 and data collectors 28 are linked to the central control center. The control center aggregates traffic information and coordinates measures to track down and block the sources of an attack.**

Cox discloses analyzing packets not statistics. Fletcher although clearly directed to collection of statistics and transfer of network packets, fails to suggest how to use the collected statistics in an arrangement to thwart an attack on a victim data center. Fletcher thus fails to suggest how analyzing network traffic statistics to identify malicious network traffic and filtering the network traffic based on results of analyzing the network traffic could occur given its teachings of those of Cox.

Therefore, it would not be obvious to one of ordinary skill in the art to combine the teachings of Cox with Fletcher, since neither reference suggests how the stand-alone arrangement disclosed in Cox could be modified to the distributed arrangement of Fletcher. Thus, the combination of Fletcher and Cox is not suggested. Assuming *arguendo* that such a combination was suggested, the suggested combination of Fletcher and Cox still fails to suggest all of the features of claim 1.

According, neither Fletcher nor Cox nor the newly cited art suggest the combination of features in claim 1.

Claims 2-11 add additional distinguishing features. Claim 2, for instance recites arranging the monitors and central controller to be coupled to the redundant network that is

inaccessible to the denial of service attack. Neither Fletcher nor Cox disclose this feature, since Fletcher discloses using the, e.g., routing device interconnecting the private network to the public network to transmit data among collectors.

Claim 3 further distinguishes, since although claim 3 includes monitoring network traffic at an edge of the network to protect the data center, (as arguably is taught by Cox) Cox clearly neither describes nor suggests at least the feature that monitoring uses a gateway *** coupled to the control center by the redundant network. Neither Cox nor Fletcher discloses or suggests the control center.

Claim 6 further limits claim 1 and recites performing intelligent traffic analysis based on collected statistical data from the monitors and filtering further comprises filtering the traffic according to the traffic analysis to eliminate the traffic identified as part of the denial of service attack. Claims 7 and 8 further limit claim 6 and distinguish by specifying that gateways and the control center performing intelligent traffic analysis (claim 7) or the gateways perform the analysis (claim 8).

Claim 9 which limits claim 1 distinguishes since, neither reference suggests monitoring network traffic by data collectors sampling packet traffic and accumulating and collecting statistical information about network flows and aggregating packet traffic and accumulated statistical information in the control center to coordinate measures to track down and block the sources of an attack.

Claim 11 distinguishes since the references neither describe nor suggest aggregating traffic information in the control center to coordinate measures to track down and block the sources of an attack.

Claim 12 distinguishes over Fletcher and Cox since the references neither describe nor suggest the combination of a distributed system to thwarting denial of service attacks, including a plurality of monitors dispersed throughout a network, the monitors collecting statistical data for performance of intelligent traffic analysis and filtering to identify malicious traffic and to eliminate the malicious traffic to thwart the denial of service attack. Fletcher does not have teachings directed to denial of service attacks and it would not be obvious to one of ordinary skill

in the art to combine the teachings of Cox with Fletcher, since neither reference suggests how the stand-along arrangement disclosed in Cox could be modified to the distributed arrangement of Fletcher.

Claims 13-14 recite additional features not suggested by the combination of references

Claims 15-27 are allowable for reasons analogous to those given for claim 1 and corresponding ones of claims 2-11.

Claim 28 directed to a distributed system to thwart denial of service attacks including a plurality of gateways dispersed throughout a network, near data centers that might be sources of an attack, the gateways collecting statistical data for performance of intelligent traffic analysis and filtering, identify malicious traffic at the source of an attack, to eliminate the malicious traffic and thwart the denial of service attack, is allowable for analogous reasons as in claim 15, except that claim 28 is limited to gateways.

Claims 29-36 add additional allowable features.

The examiner provisionally rejected claims 1, 4, 6, 8, 12, 15, and 28 under the judicially created doctrine of obvious type double patenting in view of co-pending application serial no. 10/062,974.

Neither claims 1, 4, 6, 8, 12, 15, and 28 nor the remaining claims in the instant application claim the same invention as claims 1, 8, 15, 17, 20, 22 and 24 of co-pending application serial no. 10/062,974. Claim 1 of the instant application recites:

> 1. (currently amended) A method of thwarting denial of service attacks on a victim data center coupled to a network, the method comprising:
>
> monitoring network traffic through monitors disposed at a plurality of points in the network; and
>
> communicating data from the monitors to a central controller, over a redundant network that is a different network from the network being monitored.

Original claim 8 of the co-pending application, recites:

8. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

monitoring network traffic through probes that are disposed between the victim data center and the network; and

communicating data from the probes, over a dedicated network, to a cluster head device.

Currently amended claim 8 of the co-pending application, recites:

8. (Currently Amended) A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

monitoring network traffic through probes that are disposed to monitor packets over links that couple the victim data center and the network; and

communicating data from the probes, over a dedicated network, to a cluster head device.

Claim 1 of the instant application requires monitoring with monitors disposed at a plurality of points in the network, with the monitors communicating data to a central controller. In contrast, Claim 8, (as originally filed) of the co-pending application requires monitoring through probes that are disposed between the victim data center and the network, with the probes communicating data to a cluster head device, and claim 8 as amended requires monitoring network traffic through probes that are disposed to monitor packets over links that couple the victim data center and the network. Claims 1 and 8 (either original or as amended) do not claim the same invention, nor do these claims claim obvious variations.

The monitors (or probes) in claims 1 of the instant application and 8 of the co-pending application are disposed in different locations. In claim 1, the monitors are disposed at a plurality of points in the network, whereas, in claim 8, the probes are disposed between the victim data center and the network (to monitor links between the data center and the network). Additionally, the probes (claim 8) communicate with the cluster head, whereas in claim 1 of the instant application the monitors communicate with the central controller. A central controller is described in both applications, whereas the cluster head is not described in the instant case. The

central controller is not the same element as a cluster head shown in FIG. 3 of the co-pending application, but is not shown in any of the figures of the instant application. Similar arguments apply for the other claims.

The clusterhead and central controller are distinguishable since the central controller receives data from data collectors disposed in a "plurality of points in the network" e.g., traffic for multiple data centers, whereas the clusterhead/probe arrangement of claim 8 allows visibility into multiple links at one physical location, e.g., data center.

Claims 1 and 8, as well as the other claims, therefore claim inventions that are distinct from one another. Consequently, the double patenting rejection under obviousness type double patenting is improper.

Applicant has enclosed an Information Disclosure Statement. Applicant contends that the references enclosed neither describe nor suggest the features of Applicant's invention whether taken alone or in combination with the art of record.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 7/26/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21096094.doc